



June 18, 2021

VIA ELECTRONIC FILING

The Honorable Jocelyn Boyd
Public Service Commission of South Carolina
101 Executive Center Drive
Columbia, South Carolina 29211

RE: Dominion Energy South Carolina, Inc.;
Request for Approval of Contract to Acquire the Fort Jackson Natural
Gas Distribution
Docket No. 2019-108-G

Dear Ms. Boyd:

By Order No. 2019-272, dated April 17, 2019, the Public Service Commission of South Carolina ("Commission") approved a contract between Dominion Energy South Carolina, Inc. ("DESC" or "Company") and the United States Department of Defense ("DoD"), through its contracting agent Defense Logistics Agency Energy FEE - Utility Services, pursuant to which DESC acquired and now operates the natural gas distribution system serving Fort Jackson located in Richland County, South Carolina.

The purpose of this letter is to inform the Commission that DESC and the DoD have executed a twelfth and thirteenth amendment which modifies certain terms of the original contract (the "Twelfth Amendment" and the "Thirteenth Amendment"). The Twelfth Amendment is attached to this letter as Exhibit A and identified as P00012. The Thirteenth Amendment is attached to this letter as Exhibit B and identified as P00013.

Beginning with the Twelfth Amendment, this amendment funds the Gross Receipt Tax and the Public Service Commission fee for the time period November 19, 2019 to October 18, 2020. As a result of this change, the Twelfth Amendment also establishes accounting classification reference number AN ("ACRN AN"). A summary of these updated charges for these matters is located on Exhibit A, Page 2,

Section B with detailed updated charges appearing on Exhibit A, Pages 2-3, Sections B and C.

Turning to the Thirteenth Amendment, this amendment address cybersecurity requirements. More specifically, the Thirteenth Amendment incorporates Defense Federal Acquisition Regulation System ("DFARS") clause 252.204-7020 NIST SP 800-171 *DoD Assessment Requirements* (Nov 2020). This amendment also deletes and replaces DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* (OCT 2016) with DFARS clause 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* (Dec 2019). A summary of these revisions is located on Exhibit B, Page 2, Section A and B. The full text of these modifications is set forth on Exhibit B, pages 2 – 10.

No Commission approval is required of these amendments, but the Company is filing the amendments with the Commission to ensure that its administrative file is current.

If you have any questions or need additional information, please do not hesitate to contact us.

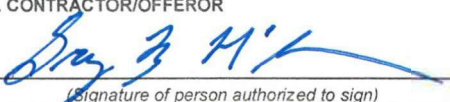
Very truly yours,



K. Chad Burgess

KCB/tmh

cc: Jeffrey M. Nelson, Esquire
(via electronic and U.S. Mail w/enclosures)

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE K		PAGE 1 OF 3 PAGES	
2. AMENDMENT/MODIFICATION NUMBER P00012		3. EFFECTIVE DATE See Block 16C		4. REQUISITION/PURCHASE REQUISITION NUMBER	
5. PROJECT NUMBER (If applicable)					
6. ISSUED BY DEFENSE LOGISTICS AGENCY ENERGY 8725 JOHN J. KINGMAN ROAD, STP 10400 FORT BELVOIR, VA 22060-6221 Buyer/Symbol: Jonathan Willsher / DLA-Energy FEEAB Phone: (571) 767-9760 Email: jonathan.willsher@dla.mil P.P. : 8.2		7. ADMINISTERED BY (If other than Item 6)		CODE	
8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code) Dominion Energy South Carolina, Inc. DUNS # 007919517 220 Operations Way MC J50 Cayce, SC, 29033 POC: Greg B. McGlohorn Email: greg.mcglhorn@dominionenergy.com Phone: (803) 217-7346		(X)		9A. AMENDMENT OF SOLICITATION NUMBER	
		<input type="checkbox"/>		9B. DATED (SEE ITEM 11)	
		<input checked="" type="checkbox"/>		10A. MODIFICATION OF CONTRACT/ORDER NUMBER SP0600-18-C-8326	
		<input checked="" type="checkbox"/>		10B. DATED (SEE ITEM 13) September 28, 2018	
CODE 1DQY6		FACILITY CODE:			
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS					
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers <input type="checkbox"/> is extended. <input type="checkbox"/> is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.					
12. ACCOUNTING AND APPROPRIATION DATA (If required) See Section G, Accounting and Appropriation Data.					
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.					
CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A.				
<input type="checkbox"/>					
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).				
<input checked="" type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: DFARS 252.232-7007 Limitation of Government's Obligation				
<input type="checkbox"/>	D. OTHER (Specify type of modification and authority)				
E. IMPORTANT: Contractor <input type="checkbox"/> is not <input checked="" type="checkbox"/> is required to sign this document and return <u>1</u> copies to the issuing office.					
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)					
Fort Jackson, SC – Utility Services Contract Natural Gas Distribution System See Additional Pages for further Details.					
Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.					
15A. NAME AND TITLE OF SIGNER (Type or print) Greg B. McGlohorn - General Manager, Gas Operations			16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Vicki L. Warner, Contracting Officer DLA Energy FEEAB		
15B. CONTRACTOR/OFFEROR  (Signature of person authorized to sign)		15C. DATE SIGNED 4-16-21		16B. UNITED STATES OF AMERICA WARNER.VICKI.L.121282032 2 Digitally signed by WARNER.VICKI.L.121282032 Date: 2021.04.23 11:53:35 -04'00'	
				16C. DATE SIGNED 4/23/21	
				(Signature of Contracting Officer)	

SP0600-18-C-8326
Modification P00012

Fort Jackson, SC
Page 2 of 3

A. The purpose of this modification is to:

1. Fund the Gross Receipt Tax (GRT) and Public Service Commission (PSC) Fee for contract SP0600-18-C-8326 from November 19, 2019 to October 18, 2020;
2. Update Section B.3, Schedule, to fund SubCLIN 0154AA;
3. Update Section G.6, Accounting and Appropriation Data, to establish ACRN AN.

B. SECTION B – Supplies and Services and Prices/Costs – As a result of items listed in paragraph A, Section B.3 *Schedule*, is revised as follows:

CLIN 0154AA is revised as follows (changes in **bold**):

FROM:

CLIN	Description	Qty	Unit	Unit Price	Total Price
0154	GRT / PSC Fee – Transition Period of Performance: November 19, 2019 – November 18, 2020				
0154AA	GRT / PSC Fee (Months 1 – 11 of 600) – Transition Period of Performance: November 19, 2019 – October 18, 2020 ACRN: TBD	1	MO	\$1,340.00	\$1,340.00

TO:

CLIN	Description	Qty	Unit	Unit Price	Total Price
0154	GRT / PSC Fee – Transition Period of Performance: November 19, 2019 – November 18, 2020				
0154AA	GRT / PSC Fee (Months 1 – 11 of 600) – Transition Period of Performance: November 19, 2019 – October 18, 2020 ACRN: AN	1	MO	\$1,340.00	\$1,340.00

SP0600-18-C-8326
Modification P00012

Fort Jackson, SC
Page 3 of 3

C. G – Contract Administration Data – As a result of items listed in paragraph A, Section G.6 *Accounting and Appropriation Data*, is revised as follows:

ACRN AN is established in the amount of \$1,340.00. Funds are provided under Direct Fund Cite MIPR Number 11630599, Basic, provided by the installation. A funding breakdown is provided as follows:

02120202020 2020000 A60TD 131079QUTS 252G 0011630599 S.0070011.22.14 021001

Funding Breakdown:

	CLIN 0154AA	\$1,340.00
Total Funding for ACRN AN:		\$1,340.00

- D.** The total amount obligated on this contract has increased by \$1,340.00, from \$708,587.00, to \$709,927.00.
- E.** The total estimated contract value on this contract remains unchanged at \$44,548,908.00.
- F.** All other Terms and Conditions of this contract remain unchanged and in full force and effect.

End of Modification

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE K	PAGE 1	OF 11	PAGES
-----------------------	--------	-------	-------

2. AMENDMENT/MODIFICATION NUMBER P00013	3. EFFECTIVE DATE See Block 16	4. REQUISITION/PURCHASE REQUISITION NUMBER	5. PROJECT NUMBER (If applicable)
6. ISSUED BY DEFENSE LOGISTICS AGENCY ENERGY 8725 JOHN J. KINGMAN ROAD, STP 10400 FORT BELVOIR, VA 22060-6221 Phone: 571-767-9760 Email: jonathan.willsher@dla.mil	CODE SP0600	7. ADMINISTERED BY (If other than Item 6)	CODE

8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code) Dominion Energy South Carolina, Inc. 220 Operations Way MC J50 Cayce, SC, 29033 POC: Greg McGlohorn Phone: (803) 217-7346	(X) <input type="checkbox"/> <input checked="" type="checkbox"/>	9A. AMENDMENT OF SOLICITATION NUMBER 9B. DATED (SEE ITEM 11) 10A. MODIFICATION OF CONTRACT/ORDER NUMBER SP0600-18-C-8326 10B. DATED (SEE ITEM 13) September 28, 2018
CODE 1DQY6	FACILITY CODE:	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:
(a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See Section G, Accounting and Appropriation Data.

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A.
<input type="checkbox"/>	
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
<input type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
<input checked="" type="checkbox"/>	D. OTHER (Specify type of modification and authority) DFARS 204.73 Safeguarding Covered Defense Information and Cyber Incident Reporting

E. IMPORTANT: Contractor ☒ is not ☐ is required to sign this document and return 0 copies to the issuing office.**14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)**

**Fort Jackson, SC – Utilities Privatization Contract
Natural Gas Distribution System**

See Additional Pages for further Details.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Vicki L Warner Contracting Officer DLA Energy
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED
16B. UNITED STATES OF AMERICA WARNER.VICKI.L.12128 20322 Digitally signed by WARNER.VICKI.L.1212820322 Date: 2021.05.06 16:46:28 -04'00'	16C. DATE SIGNED 5/6/21 (Signature of Contracting Officer)

Previous edition unusable

STANDARD FORM 30 (REV. 11/2016)

Prescribed by GSA FAR (48 CFR)

ELECTRONICALLY FILED - 2021 June 18 9:47 AM - SCS-SC - Docket # 2019-108-G - Page 6 of 15

A. The contract is modified as follows, Section I.6 Other Clauses and Contract Text of the contract:

1. Incorporates DFARS clause 252.204-7020 NIST SP 800-171 *DoD Assessment Requirements* (Nov 2020), in full text.
2. Delete and replace DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* (OCT 2016) with DFARS clause 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* (Dec 2019), in full text.

B. SECTION I – Contract Clauses – Section I.6 *Other Clauses and Contract Text*, is updated to:

1. Incorporate DFARS clause 252.204-7020 NIST SP 800-171 *DoD Assessment Requirements* (Nov 2020) in full text, as follows:

DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements (Nov 2020)

(a) Definitions.

Basic Assessment means a contractor's self-assessment of the contractor's implementation of NIST SP 800-171 that—

- (1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);
- (2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and
- (3) Results in a confidence level of “Low” in the resulting score, because it is a self-generated score.

Covered contractor information system has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

High Assessment means an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—

- (1) Consists of—
 - (i) A review of a contractor's Basic Assessment;
 - (ii) A thorough document review;
 - (iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the contractor's system security plan; and
 - (iv) Discussions with the contractor to obtain additional information or clarification, as needed; and
- (2) Results in a confidence level of “High” in the resulting score.

Medium Assessment means an assessment conducted by the Government that—

- (1) Consists of—
 - (i) A review of a contractor's Basic Assessment;
 - (ii) A thorough document review; and

(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "Medium" in the resulting score.

(b) *Applicability.* This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, in accordance with Defense Federal Acquisition Regulation System (DFARS) clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

(c) *Requirements.* The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology

at https://www.acq.osd.mil/dpap/pdi/cyber/strategically__assessing__contractor__implementation__of__NIST__SP__800-171.html, if necessary.

(d) *Procedures.* Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) (<https://www.spr.scd.disa.mil/>) to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology to webpmsmh@navy.mil for posting to SPRS.

(i) The email shall include the following information:

(A) Version of NIST SP 800-171 against which the assessment was conducted.

(B) Organization conducting the assessment (*e.g.*, Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(1) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(2) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (*e.g.*, 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (*i.e.*, a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Contractor shall use the following format for the report:

System security plan	CAGE codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total score	Date score of 110 will achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:

- (i) The standard assessed (*e.g.*, NIST SP 800-171 Rev 1).
- (ii) Organization conducting the assessment, *e.g.*, DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).
- (iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.
- (iv) A brief description of the system security plan architecture, if more than one system security plan exists.
- (v) Date and level of the assessment, *i.e.*, medium or high.
- (vi) Summary level score (*e.g.*, 105 out of 110, not the individual value assigned for each requirement).
- (vii) Date that all requirements are expected to be implemented (*i.e.*, a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(e) *Rebuttals.*

- (1) DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide https://www.sprs.csd.disa.mil/pdf/SPRS__Awardee.pdf).
- (2) Upon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

(f) *Accessibility.*

- (1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).
- (2) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS__Awardee.pdf.
- (3) A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this clause. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act

(e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(g) *Subcontracts.*

(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, to webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.

(End of clause)

2. Delete and replace clause DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* (Oct 2016) with clause DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* (Dec 2019), in full text as follows:

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)

(a) *Definitions.* As used in this clause—

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on

Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Covered contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

- (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
- (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Operationally critical support means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

Rapidly report means within 72 hours of discovery of any cyber incident.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

SP0600-18-C-8326
Modification P00013

Fort Jackson, SC
Page 7 of 10

(b) *Adequate security.* The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (*i.e.*, other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at <http://dx.doi.org/10.6028/NIST.SP.800-171>) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (<https://www.fedramp.gov/resources/documents/>) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (*e.g.*, medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <https://dibnet.dod.mil>.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <https://dibnet.dod.mil>.

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see <https://public.cyber.mil/eca/>.

(d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) *Media preservation and protection.* When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis.* Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities.* If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information

SP0600-18-C-8326
Modification P00013

Fort Jackson, SC
Page 9 of 10

obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

- (1) To entities with missions that may be affected by such information;
- (2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
- (3) To Government entities that conduct counterintelligence or law enforcement investigations;
- (4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
- (5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts.* The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

SP0600-18-C-8326
Modification P00013

Fort Jackson, SC
Page 10 of 10

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

C. The total amount obligated on this contract remains unchanged in the amount of \$709,927.00.

D. The total estimated contract value on this remains unchanged at \$44,548,908.00.

E. All other Terms and Conditions of this contract remain unchanged and in full force and effect.

End of Modification